To Prevent

Wipe Hard Drives

Identity Theft

Crit Luallen: Auditor Alert

For Details See: www.Auditor.Ky.Gov

CRIT LUALLEN
AUDITOR OF PUBLIC ACCOUNTS

June 28, 2005

AUDITOR'S ALERT

The Auditor's Office, in the form of an Auditor's Alert, periodically offers guidance and recommendations to public officials regarding fiscal matters, accountability, and best practices.

Electronic Media Must Be Sanitized Prior To Disposal

Based on recent alarming findings, Auditor of Public Accounts Crit Luallen alerts state and local government entities of the vital importance to thoroughly sanitize information residing on computer systems or other electronic media no longer in service. The failure to sanitize a single computer could potentially place confidential information of thousands of state employees and other citizens at risk for abuse, including identity theft.

A recent analysis performed by this office of a random sample of surplused computers about to be released to the public revealed that one computer contained a substantial amount of confidential information. Specifically, this information included the names, pictures, and social security numbers of thousands of state employees and other citizens who had been issued access cards to state facilities from December 1997 through August 2002.

The Governor's Office for Technology issued on February 5, 2003, an Enterprise Policy/Procedure, CIO-077, entitled "Sanitization of Information Technology Equipment and Electronic Media." This policy remains in effect and identifies acceptable methods to sanitize a computer or other electronic media. The purpose of the policy is to ensure the appropriate sanitization of electronic media prior to disposal to prevent the release of confidential or sensitive information. Each agency is responsible to ensure its employees are aware of and comply with this policy.

This policy identifies the acceptable methods to sanitize computer hard drives and offers procedural guidance for implementation. The policy notes that computer hard drives containing sensitive or confidential information must be securely erased using the recommended Department of Defense Sanitization Procedures listed in the policy.

The Auditor's Office issued a similar alert in February 2003 that resulted in the Governor's Office for Technology developing the sanitization policy that remains in effect. This office continues to evaluate government agencies' compliance with security policies and procedures in an effort to ensure proprietary, personal, and confidential information is adequately secured.

105 SEA HERO ROAD, SUITE 2
FRANKFORT, KY 40601-5404

TELEPHONE 502.573.0050
FACSIMILE 502.573.0067
WWW.AUDITOR.KY.GOV

Office of the Chief Information Officer
ENTERPRISE POLICY/PROCEDURE

Policy Number: CIO-077

Effective Date: 2/5/2003
Revision Date: 6/10/2003

Subject: Sanitization of Information Technology Equipment and Electronic Media

Policy: The purpose of this policy is to ensure secure and appropriate disposal of information technology (IT) equipment, devices, network components, operating systems, application software and storage media belonging to the Commonwealth to prevent unauthorized use or misuse of state information. All IT equipment shall be properly sanitized prior to disposal or release and sanitization procedures shall be properly documented to prevent unauthorized release of sensitive and/or confidential information that may be stored on that equipment and other electronic media. This policy supports the Enterprise Architecture for security and privacy and outlines procedures that must be followed to protect the Commonwealth.

Policy Maintenance: The Office of the CIO has issued this Enterprise Policy. The Governor's Office for Technology (GOT), Office of Infrastructure Services, is responsible for the maintenance of this policy. This policy shall be adhered to by all agencies and employees within the Executive Branch of state government. However, agencies may choose to add to this policy, in order to enforce more restrictive policies as appropriate. Therefore, employees are to refer to their agency's internal policy, which may have additional information or clarification of this enterprise policy.

Responsibility for Compliance: Each agency is responsible for assuring that appropriate employees within their organizational authority have been made aware of the provisions of this policy, that compliance by the employee is expected, and that unauthorized and/or neglectful release of computer equipment and/or related media, especially that which contain sensitive and/or confidential information, may result in disciplinary action pursuant to KRS 18A up to and including dismissal.

It is also each Executive Cabinet's responsibility to enforce and manage this policy. Failure to comply may result in additional shared service charges to the agency for GOT's efforts to remediate issues related to lack of or improper sanitization of computer equipment and related media.

Definitions:

Clearing: The process of deleting the data on the media before the media is reused. It is important to note that clearing will allow for the retrieval of information if certain retrieval procedures are used and is not approved for computer equipment or media that contain sensitive and/or confidential data.

Coercivity: Magnetic media is divided into three types (I, II, III) based on their coercivity. Coercivity of magnetic media defines the magnetic field necessary to reduce a magnetically saturated material's magnetization to zero. The level of magnetic media coercivity must be ascertained before executing any degaussing procedure.

Degauss: Procedure that reduces the magnetic flux on media virtually to zero by applying a reverse magnetizing field. Properly applied, degaussing renders any previously stored data on magnetic media unreadable and may be used in the sanitization process. Degaussing is more effective than overwriting magnetic media.

Degausser: Device used to remove data from magnetic storage medium.

DoD Sanitization Standard (5520.22-M): US Department of Defense standard for clearing and sanitizing data on writable media.

Dynamic Random Access Memory (DRAM): The most common kind of random access memory (RAM) for personal computers and workstations. Unlike firmware chips (ROMs, PROMs, etc.) DRAM loses its content when the power is turned off.

Electronically Alterable PROM (EAPROM): A PROM whose contents can be changed.

Electronically Erasable PROM (EEPROM): User-modifiable read-only memory (ROM) that can be erased and reprogrammed (written to) repeatedly through the application of higher than normal electrical voltage. A special form of EEPROM is flash memory.

Erasable Programmable ROM (EPROM): Programmable read-only memory (programmable ROM) that can be erased and re-used. Erasure is caused by shining an intense ultraviolet light through a window that is designed into the memory chip.

Flash EPROM (FEPROM): Non-volatile device similar to EEPROM, but where erasing can only be done in blocks or the entire chip.

Programmable ROM (PROM): Read-only memory (ROM) that can be modified once by a user.

Magnetic Bubble Memory: A non-volatile memory device for computers that uses magnetic bubbles for recording bits. The technology was used in early 1980s but is obsolete today.

Magnetic Core Memory: Random access memory (RAM) system that was developed at MIT in 1951. Magnetic core memory replaced vacuum tubes and mercury delay lines with a much more compact and reliable technology. Semiconductor memories largely replaced magnetic cores in the 1970s.

Magnetic Plated Wire: Non-volatile memory created by Honeywell in 1960s. Magnetic plated wire consists of a copper conductor covered with a thin layer of highly magnetic material, over which a polyurethane insulating film is enameled.

Nonvolatile RAM (NOVRAM): Memory that does not lose its information while its power supply is turned off.

Oersteds: The unit of magnetic field strength in the centimeter-gram-second system.

Overwriting: A software process that replaces the data previously stored on magnetic storage media with a predetermined set of meaningless data. Overwriting is an acceptable method for clearing; however, the effectiveness of the overwrite procedure may be reduced by several factors, including: ineffectiveness of the overwrite procedures, equipment failure (e.g., misalignment of read/write heads), or inability to overwrite bad sectors or tracks or information in inter-record gaps.

Overwriting Procedure: The preferred method to clear magnetic disks is to overwrite all locations three (3) times (the first time with a random character, the second time with a specified character, the third time with the complement of that specified character).

Read Only Memory (ROM): Built-in" computer memory containing data that normally can only be read, not written to. The data in ROM is not lost when the computer power is turned off. The ROM is sustained by a small long-life battery in your computer.

Sanitizing: The process of removing the data on the media before the media is reused in an environment that does not provide an acceptable level of protection for the data. In general, laboratory techniques cannot retrieve data that has been sanitized/purged. Sanitizing may be accomplished by degaussing.

Static Random Access Memory (SRAM): Random access memory (RAM) that retains data bits in its memory as long as power is being supplied. SRAM is used for a computer's cache memory and as part of the random access memory digital-to-analog converter on a video card.

Procedures:

1.0 Sanitization of IT Equipment and Electronic Media

The sale, transfer, or disposal of computers, computer peripherals, and computer software or other IT devices can create information security risks for the Commonwealth. These risks are related to potential violation of software license

agreements, unauthorized release of sensitive and/or confidential information, and unauthorized disclosure of trade secrets, copyrights, and other intellectual property that might be stored on the hard disks and other storage media. It should be noted that computers containing sensitive and/or confidential data must have their hard drives securely erased as specified by the US Department of Defense (DoD) standards listed in section 1.4 – Recommended DoD Sanitation Procedures.

The following procedures must be followed when a computer system is sold, transferred, or disposed of. This policy does not supersede specific policies, directives or standards required by federal or state agencies pertaining to the disposal of computer equipment. The following procedures also apply to contractor-supplied computers.

- Before a computer system is sold, transferred, or otherwise disposed of, all sensitive and/or confidential program or data files on any storage media must be completely erased or otherwise made unreadable in accordance with DoD standards (5220.22-M) unless there is specific intent to transfer the particular software or data to the purchaser/recipient.

- The computer system must be relocated to a designated, secure storage area until the data can be erased.

- Hard drives of surplus computer equipment must be securely erased within 60 days after replacement.

- Whenever licensed software is resident on any computer media being sold, transferred, or otherwise disposed of, the terms of the license agreement must be followed.

After the sanitization of the hard drive is complete, the process must be certified and a record maintained as specified by the agency's records retention schedule.

1.1 Sanitization of Hard Drives

The following section outlines the acceptable methods to expunge data from storage media. Sanitization must be performed on hard drives to ensure that information is removed from the hard drive in a matter that gives assurance that the information cannot be recovered. Before the sanitization process begins, the computer must be disconnected from any network to prevent accidental damage to the network operating system or other files on the network.

There are three acceptable methods to be used for the sanitization of hard drives:

- Overwriting

- Degaussing
- Physical Destruction

The method used for sanitization, depends upon the operability of the hard drive:

- Operable hard drives that will be reused must be overwritten prior to disposition. If the operable hard drive is to be removed from service completely, it must be physically destroyed or degaussed.

- If the hard drive is inoperable or has reached the end of its useful life, it must be physically destroyed or degaussed.

Clearing data (deleting files) removes information from storage media in a manner that renders it unreadable unless special utility software or techniques are used to recover the cleared data. However, because the clearing process does not prevent data from being recovered by technical means, it is not an acceptable method of sanitizing state owned hard disk storage media.

1.1.1 Overwriting Specifications

Overwriting is an approved method for sanitization of hard disk drives. Overwriting of data means replacing previously stored data on a drive or disk with a predetermined pattern of meaningless information. This effectively renders the data unrecoverable. All software products and applications used for the overwriting process must meet the following specifications:

- The data must be properly overwritten with a pattern. GOT requires overwriting with a pattern, and then its complement, and finally with a random pattern of 1's and 0's.

- Sanitization is not complete until three overwrite passes and a verification pass is completed.

- The software must have the capability to overwrite the entire hard disk drive, independent of any BIOS or firmware capacity limitation that the system may have, making it impossible to recover any meaningful data.

- The software must have the capability to overwrite using a minimum of three cycles of data patterns on all sectors, blocks, tracks, and any unused disk space on the entire hard disk medium.

- The software must have a method to verify that all data has been removed.

- Sectors not overwritten must be identified.

1.1.2 Degaussing Specifications

Degaussing is a process whereby the magnetic media is erased. Hard drives seldom can be used after degaussing. The degaussing method should only be used when the hard drive is inoperable and will not be used for further service.

Please note that extreme care should be used when using degaussers since this equipment can cause extreme damage to nearby telephones, monitors, and other electronic equipment. Also, the use of a degausser does not guarantee that all data on the hard drive will be destroyed. Degaussing efforts should be audited periodically to detect equipment or procedure failures.

The following standards and procedures must be followed when hard drives are degaussed:

- Follow the product manufacturer's directions carefully. It is essential to determine the appropriate rate of coercivity for degaussing.

- Shielding materials (cabinets, mounting brackets), which may interfere with the degausser's magnetic field, must be removed from the hard drive before degaussing.

- Hard disk platters must be in a horizontal direction during the degaussing process.

1.1.3 Physical Destruction

Hard drives must be destroyed when they are defective or cannot be repaired or sanitized for reuse. Physical destruction must be accomplished to an extent that precludes any possible further use of the hard drive. This can be attained by removing the hard drive from the cabinet and removing any steel shielding materials and/or mounting brackets and cutting the electrical connection to the hard drive unit. The hard drive should then be subjected to physical force (pounding with a sledge hammer) or extreme temperatures (incineration) that will disfigure, bend, mangle or otherwise mutilate the hard drive so it cannot be reinserted into a functioning computer.

1.2 Sanitization of Other Computer Media

If there is any risk of disclosure of sensitive data on media other than computer hard drives, the appropriate sanitization methods as outlined in the DoD recommended sanitization procedures should be followed. Particular attention should be paid to floppy disks, tapes, CDs, DVDs, and optical disks.

Memory components should also be sanitized before disposal or release. Memory components reside on boards, modules, and sub-assemblies. A board can be a module, or may consist of several modules and sub-assemblies.

Unlike magnetic media sanitization, clearing may be an acceptable method of sanitizing components for release. Memory components are categorized as either volatile or nonvolatile, as described below. DoD Sanitization Procedures should be followed as specified in section 1.4

Volatile memory components *do not* retain data after removal of all electrical power sources, and when re-inserted into a similarly configured system do not contain residual data, i.e. SRAM, DRAM.

Nonvolatile memory components *do* retain data when all power sources are discontinued. Nonvolatile memory components include Read Only Memory (ROM), Programmable ROM (PROM), or Erasable PROM (EPROM) and their variants. Memory components that have been programmed at the vendor's commercial manufacturing facility and are considered unalterable in the field may be released; otherwise, DoD Sanitization Procedures must be followed.

1.3 Certification of Sanitization

Sanitization may be required in instances other than surplusing. It is recommended that a record is kept for all sanitization procedures, it is required when equipment is surplused. Prior to submitting surplus forms (B217-2: Declared Surplus) from Finance and Administration, Division of Surplus Property) to the agency's appropriate organizational unit, the sanitizing process must be documented on an additional form that explicitly outlines the method(s) used to expunge the data from the storage media, the type of equipment/media being sanitized, the name of the individual requesting sanitization, and the name of the person responsible for the sanitization A template for the form is attached at the end of this policy, Commonwealth of Kentucky Record of IT Equipment Sanitization. Its lower portion contains the elements required by the Division of Surplus Property. A completed record (including the top section) must be maintained in a central location designated by the agency. This information must be maintained as outlined by the Kentucky Department of Library and Archives (KDLA) record retention schedule.

The Finance and Administration Division of Surplus Property requires that a copy of the proof of sanitization accompany all hard drives earmarked for disposal. This proof may be a copy of the entire "Record of IT Equipment Sanitization" or of the lower portion of the form. In instances where attaching the paper form to the equipment is a poor method, a label containing the required information may be affixed to the hard drive(s), equipment case (e.g., CPU box) or appropriate surface. The label must contain the name and signature of the person performing the sanitization, equipment identification and sanitization method used as provided in the lower portion of the "Record of IT Equipment Sanitization". Equipment Serial and Inventory numbers must match those on the B217-2 form and a copy of the record should be attached to the B217-2 as an attachment to provide the "Agency Explanation of Loss or Destruction".

For disposition other than to the Division of Surplus Property (such as interagency transfer), it is highly recommended that an adhesive label be affixed

to the equipment case to record the sanitization process before transfer. Questions remain about leased equipment and equipment maintained through a service agreement. Agencies must assess liability on a case by case review.

1.4 Recommended DoD Sanitization Procedures

Media	Procedure(s)
Magnetic Tape	
Type I*	a, b, or m
Type II**	b or m
Type III***	m
Magnetic Disk	
Bernoullis	m
Floppies	m
Non-Removable Rigid Disk	a, b, d, or m
Removable Rigid Disk	a, b, d, or m
Optical Disk	
Read Many, Write Many	m
Read Only	m, n
Write Once, Read Many (WORM)	m, n
Memory	
Dynamic Random Access Memory (DRAM)	c, g, or m
Electronically Alterable PROM (EAPROM)	j or m
Electronically Erasable PROM (EEPROM)	h or m
Erasable Programmable ROM (EPROM)	l, then c or m
Flash EPROM (FEPROM)	c, then I or m
Programmable ROM (PROM)	m
Magnetic Bubble Memory	a, b, c, or m
Magnetic Core Memory	a, b, e, or m
Magnetic Plated Wire	c and f, or m
Magnetic Resistive Memory	m
Nonvolatile RAM (NOVRAM)	c, g, or m
Read Only Memory (ROM)	m
Static Random Access Memory (SRAM)	c and f, g, or m

Sanitization Procedure Key

a. Degauss with a Type I degausser.
b. Degauss with a Type II degausser.
c. Overwrite all addressable locations with a single character.
d. Overwrite all addressable locations with a character, its complement, then a random character and verify. THIS METHOD IS NOT APPROVED FOR SANITIZING MEDIA THAT CONTAINS EXTREMELY CONFIDENTIAL OR SENSITIVE INFORMATION.

e. Overwrite all addressable locations with a character, its complement, and then a random character.
f. Each overwrite must reside in memory for a period longer than the classified data resided.
g. Remove all power to include battery power.
h. Overwrite all locations with a random pattern, all locations with binary zeros, all locations with binary ones.
i. Perform a full chip erase as per manufacturer's data sheets.
j. Perform i. above, then c. above, three times.
k. Perform an ultraviolet erase according to manufacturer's recommendation.
l. Perform k above, but increase time by a factor of three.
m. Destroy – disintegrate, incinerate, pulverize, shred, or melt.
n. Destruction required only if classified information is contained.

This information was extracted from the US Department of Defense 5220.22-M Clearing and Sanitization Matrix.

*Type 1 magnetic tape includes all tapes with a coercivity factor (amount of electrical force required to reduce the recorded magnetic strength to zero) not exceeding 350 oersteds.
**Type 2 magnetic tape includes all tapes with a coercivity factor between 350 and 750 oersteds.
***Type 3 magnetic tape commonly referred to as high-energy tape (4 or 8mm tape are examples), includes all tapes with a coercivity factor between 750 and 1700.

Commonwealth of Kentucky Record of IT Equipment Sanitization

Date Requested: _____

Agency (include Cabinet, Department & Division): _____

Person Submitting Request: _____

Equipment Serial Number: _____

Equipment Inventory Number: _____

Equipment Manufacturer/Model: _____

Equipment/Media Type:

- ☐ Server
- ☐ Workstation: Assigned to (name of user): _____
- ☐ Magnetic Tape (Type I, II or III)
- ☐ Magnetic Disk (Bernoulli, floppy, non-removable rigid disk, removable rigid disk)
- ☐ Optical Disk (read many-write many, read only, write once-ready many (WORM)
- ☐ Memory (DRAM, PROM, EAPROM, EPROM, FEPROM, ROM, SRAM etc.)
- ☐ Cathode Ray Tube (CRT)
- ☐ Printer
- ☐ Other (describe) _____

Disposition:

☐ Transfer ☐ Surplus ☐ Donation ☐ Repair/maintenance
☐ Return to Contractor ☐ Other (explain) _____

Decommissioning provisions:

- ☐ Equipment/media has been kept in continuous physical protection until sanitization
- ☐ Information requiring archiving as public records identified and preserved
- ☐ Temporary backups made (e.g., for equipment scheduled for repair)
- ☐ OEM operating system and other software available for reload for repurposed equipment
- ☐ MARS Fixed Asset documents completed
- ☐ Agency asset management procedures completed
- ☐ B217-2 form completed (Finance & Administration: Declared Surplus)
- ☐ Compliant with procedures for disposal of hazardous waste if destroyed
- ☐ Other (describe) _____

General description of data residing on equipment/media to be sanitized:

_____

_____

_____

Agency (Cabinet, Department & Division): _____

Person Performing Sanitization: _____

Title: _____ Date Completed: _____

Equip. Inventory #: _____ Equip. Serial #: _____

Signature: _____

Sanitization Method Used:

- ☐ DoD-compliant Overwrite (list software used): _____
- ☐ Type I Degausser
- ☐ Type II Degausser
- ☐ Full Chip Erase
- ☐ Ultraviolet Erase
- ☐ Physical Destruction (disintegrate, incinerate, pulverize, shred, melt)
- ☐ Other (describe) _____